CLAIMS

1. A data processing system which initially stores a contents ciphering key applicable to a contents ciphering process as a header data corresponding to said contents data and then executes a process for ciphering the corresponding contents data by applying said contents ciphering key contained in said header data; wherein

said header data comprises a plurality of ciphered contents ciphering key generated by said contents ciphering key respectively ciphered by applying mutually different key ciphering key.

2. The data processing system according to Claim 1, wherein

said mutually different key ciphering key comprises:

an updating key on such path for constituting a key tree structure comprising of a plurality of keys disposed in correspondence with a plurality of roots, nodes, and leaves on said paths ranging from said roots to said leaves of said key tree, wherein said individual leaves comprise a plurality of devices;

an enabling key block distribution key enciphering key respectively comprising of key enciphering key ciphered by said enabling key block containing such data for ciphering upper-rank key by means of lower-ran key; and

a storage key proper to individual storage device for storing contents data.

3. The data processing system according to Claim 2, wherein

each of said enabling key block containing said enabling key block distribution key enciphering key is so structured that, among a plurality of devices constituting leaves of said key tree structure, only such properly licensed devices are enabled to decode said enabling key block, whereas such improper devices devoid of a proper license are unable to decode said enabling key block.

4. The data processing system according to Claim 2, wherein said header further comprising:

an identification data for discerning actual storage or absence of storage of said enabling key blocks.

5. The data processing system according to Claim 1 or 2, further comprising:

a storage device for storing said header data and such contents data disposed in correspondence with said header data; and

a plurality of reproduction apparatuses for reproducing such contents data stored in said storage devices; wherein

said reproduction apparatus selects one of said ciphered plural contents ciphering keys to execute a process for ciphering said contents data.

6. The data processing system according to Claim 2, wherein

said enabling key block distribution key enciphering key to be provided after being ciphered by said enabling key block is subject to control of a version to enable a process for renewing every version to be executed.

7. The data processing system according to Claim 1, further comprising:

a storage device for storing contents data and such contents data disposed in correspondence with said header data; and

a plurality of reproduction apparatuses for reproducing a contents data stored in said storage device; wherein

each of said reproduction apparatuses functions itself as one of leaves for constituting said key tree structure by way of the following: initially, among a key tree structure comprising a plurality of reproduction apparatuses as own leaves and containing a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure,

each reproduction apparatus ciphers a specific leaf-key disposed in correspondence with own leaves by means of a storage key proper to the reproduction apparatus, and

then stores said ciphered storage key in a memory means inside of each of said reproduction apparatuses.

8. The data processing system according to Claim 1, further comprising:

a storage device for storing said header data and such contents data disposed in correspondence with said header data; and a plurality of devices for reproducing a contents data stored in said storage device; wherein

each of said devices functions itself as one of leaves for constituting said key tree structure by way of the following: initially, among a key tree structure comprising a plurality of devices as own leaves and containing a variety of keys set in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure, each of said devices stores such a leaf identification element set in correspondence with own leaves in a memory means inside of each of said reproduction apparatuses.

9. The data processing system according to Claim 1, further comprising

a storage device for storing said header data and a contents data disposed in correspondence with said header data; and

a plurality of reproduction apparatuses individually reproducing a contents data stored in said storage device; wherein

each of said reproduction apparatuses functions itself as one of leaves of said key tree structure by way of the following: initially, among a key tree structure comprising a plurality of reproduction apparatuses and containing a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure,

each of said reproduction apparatuses ciphers such a leaf-key disposed in correspondence to own leaves by applying a storage key proper to each reproduction apparatus, and

then stores said ciphered storage key in a memory means inside of a corresponding reproduction apparatus;

wherein said storage key proper to each reproduction apparatus is generated based on a leaf-identifying element of a leaf component corresponding to each reproduction apparatus present in said key tree structure.

10. The data processing apparatus according to Claim 1, further comprising:

a storage device for storing said header data and such contents data disposed in correspondence with said contents data; and

a plurality of reproduction apparatuses individually reproducing contents data stored in said storage device; wherein each of said reproduction apparatuses functions itself as one of leaves for constituting said key tree structure by way of the following: initially, among a key tree structure comprising a plurality of reproduction apparatuses and containing a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure, based on a leaf key set in correspondence with own leaves, stores a device key block in a memory means inside of each reproduction apparatus, wherein said device key block comprises an assemblage of ciphered keys comprising plural steps of node keys which are disposed on such paths ranging from own leaves up to upper rank keys of said key tree structure and individually ciphered.

11. The data processing system according to Claim 1, further comprising:

a storage device for storing said header data and such contents data disposed in correspondence with said header data; and

a plurality of reproduction apparatuses for reproducing said contents data stored in said storage device; wherein each of said reproduction apparatuses stores a plurality of initial enabling key blocks in a memory means inside of each reproduction apparatus; wherein each of said initial enabling key blocks comprises a plurality of keys on such paths for constituting a key tree structure consisting of a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure comprising a plurality of reproduction apparatuses as own leaves.

12. The data processing system according to Claim 11, wherein

each of said initial enabling key block is commonly stored in such a device belonging to lower-rank of a plurality of category nodes disposed at a predetermined step of said key tree structure.

13. A method of processing data comprising an initial step of storing a plurality of contents ciphering keys usable for ciphering a contents data in a storage device as a header data corresponding to said contents data and an ensuing step of ciphering the corresponding contents data by applying one of said contents ciphering keys present in said header data, wherein

said header data is stored in said storage device; wherein said header data includes a plurality of ciphered contents ciphering keys generated via a process for ciphering said contents ciphering keys by applying mutually different key ciphering keys.

14. The method of processing data according to Claim 13, wherein

said mutually different key ciphering keys comprise:

a plurality of updating keys on such paths for constituting a key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree comprising a plurality of devices as own leaves;

a plurality of enabling key blocks individually comprising a key enciphering key ciphered by said enabling key blocks comprising data for ciphering lower-rank keys by applying upper-rank keys; and

a storage key proper to a storage device for storing contents data therein.

15. The method of processing data according to Claim 14, wherein, among a plurality of devices constituting leaves of said key tree structure,

each of said enabling key blocks including said enabling key block distribution key enciphering key solely enables those devices qualified with a proper license to decode said enabling key block distribution key enciphering key, whereas each of said enabling key blocks prevents those devices devoid of a proper license from decoding said enabling key block distribution key enciphering key.

16. The method of processing data according to Claim 14, wherein

said header data includes such an identification data for disceming actual storage or absence of storage of said enabling key block distribution key enciphering key.

17. The method of processing data according to Claim 13 or 14, wherein, in

the process for reproducing a contents data from a storage device storing said header data and such a contents data disposed in correspondence with said header data,

said data processing method selects one of said ciphered plural contents ciphering keys to acquire a proper contents ciphering key before eventually decoding said contents data by applying said acquired contents ciphering key.

18. The method of processing data according to Claim 14, wherein, in the process for reproducing a contents data from a storage device storing said header data and such a contents data disposed in correspondence with said header data,

said data processing method executes serial processing steps including the following: initially, based on such a leaf-key disposed in correspondence with own leaves among a key tree structure comprising a variety of keys set in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure comprising a plurality of devices as own leaves, said data processing method executes:

a device key block processing step for acquiring a specific node key via a process for decoding a device key block comprising an assemblage of ciphered keys consisting of plural steps of individually ciphered mutually different node keys on such paths ranging from own leaves up to upper-rank keys of said key tree structure; and

a final step of processing said enabling key blocks based on the acquired node key.

19. A data processing apparatus for executing recording or reproduction of contents data comprising:

a system for initially storing a contents key usable for ciphering a contents data to be stored in a storage device into said storage device as a header data corresponding to said contents data followed by a step of ciphering said corresponding contents data by applying said contents key present in said header data; wherein

said data processing apparatus further executes a process for storing such header data including a plurality of ciphered contents keys individually ciphered by mutually different key enciphering keys into said storage device .

20. The data processing apparatus according to Claim 19, wherein

said mutually different key enciphering keys comprises:

a plurality of enabling key block distribution key enciphering keys individually corresponding to such key enciphering keys which are respectively ciphered by corresponding enabling key blocks including ciphering processing data for ciphering updating keys and upper-rank keys via lower-rank keys on such paths for constituting a key tree structure comprising a variety of keys respectively disposed in correspondence with such roots, nodes, and leaves on such paths ranging from roots and leaves of said key tree structure comprising a plurality of data processing apparatuses as own leaves; and

a storage key proper to a storage device for storing contents data.

21. The data processing apparatus according to Claim 20, wherein among a plurality of data processing apparatuses for constituting leaves of said key tree structure,

said enabling key block including said enabling key block distribution key enciphering key solely enables such data processing apparatuses qualified with a proper license to decode said enabling key block distribution key enciphering key, whereas said enabling key block distribution key enciphering key prevents such data processing apparatuses devoid of a proper license from decoding said enabling key block distribution key enciphering key.

22. The data processing apparatus according to Claim 20, wherein

said header data further includes such an identification element for discerning actual storage and absence of storage of said enabling key block distribution key enciphering key.

23. The data processing apparatus according to Claim 19 or 20, wherein said data processing apparatus further comprises;

such a system for executing reproduction of contents data stored in such a storage device which stores said header data and such a contents data disposed in correspondence with said header data; and

such a system which, by way of selecting one ciphered plural contents ciphering keys contained in said header data, acquires a contents key, and then decodes said contents data by applying said acquired contents key.

24. The data processing apparatus according to Claim 19, wherein said data processing apparatus further comprises:

such a system for reproducing such a contents data stored in a storage device for storing said header data and such a contents data disposed in correspondence with said header data; and

such a system which enables such a leaf-key disposed in correspondence with own leaves among a key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure comprising a plurality of data processing apparatuses as own leaves to be ciphered by a storage key proper to said data processing apparatus and then stored in a memory means inside of said corresponding data processing apparatus.

25. The data processing apparatus according to Claim 19, wherein said data processing apparatus further comprises:

such a system for executing reproduction of a contents data stored in a storage device for storing said header data and such a contents data disposed in correspondence with said header data; and

such a system for enabling a leaf identifying element disposed in correspondence with own leaves among such a key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure comprising a plurality of data processing apparatuses as own leaves to be stored in a storage device inside of said corresponding data processing apparatus.

26. The data processing apparatus according to Claim 19, wherein said data processing apparatus further comprises:

such a system for executing reproduction of contents data stored in a storage device for storing said header data and such a contents data disposed in correspondence with said header data; and

such a system for enabling a leaf key disposed in correspondence with own leaves among such a key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure comprising a plurality of data processing apparatuses as own leaves to be ciphered by applying a storage key proper to said corresponding data processing apparatus and then stored in a memory means of said data processing apparatus; wherein

said storage key proper to said corresponding data processing apparatus is generated based on a leaf-identifying element of such a leaf corresponding to said data processing apparatus present in said key tree structure.

27. The data processing apparatus according to Claim 19, wherein said data processing apparatus further comprises:

such a system for executing reproduction of a contents data stored in a storage device which stores said header data and such a contents data disposed in correspondence with said header data; and

such a system which, based on such a leaf-key provided in correspondence with own leaves among a key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure comprising a plurality of data processing apparatuses as own leaves, enables such a device key block as an assemblage of ciphered keys comprising plural steps of individually ciphered mutually different node keys on such paths ranging from own leaves up to leaves of said key tree structure to be stored in a memory means inside of said corresponding data processing apparatus.

28. The data processing apparatus according to Claim 19, wherein said data processing apparatus further comprises:

such a system for executing reproduction of a contents data stored in a storage device which stores said header data and such a contents data disposed in correspondence with said header data; and

such a system for enabling an initial enabling key block comprising a plurality of keys ciphered by means of lower rank keys on such paths for constituting a key tree structure comprising a variety keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from root to leaves of said key tree structure comprising a plurality of data processing apparatuses as own leaves to be stored in said corresponding data processing apparatus.

29. A program providing medium which enables a plurality of contents ciphering keys usable for ciphering contents data to be stored in a storage device as header data corresponding to contents data, and yet, provides a computer program which enables a process for ciphering corresponding contents data to be executed on a computer system by applying said contents ciphering key present in said header data; wherein said computer

program comprises:

a step of ciphering said contents ciphering keys by applying mutually different key enciphering keys; and

a step of enabling said header data including a plurality of ciphered contents ciphering keys generated via said preceding step for ciphering corresponding keys.